

The Onopticon: An Ontological and Methodological Analysis of Algorithmic Power from Surveillance to Environment Configuration

Hakkı Tan

Abstract

Surveillance studies in the social sciences have long been structured around Michel Foucault's model of the Panopticon. However, with the rise of digital platforms, large-scale data infrastructures, machine learning, and predictive systems, this model has become increasingly insufficient for explaining contemporary algorithmic power. This article argues not that surveillance has disappeared, but that it has reached its goal and changed form. To conceptualize this transformation, it proposes a new ontological framework: the Onopticon. The Onopticon is not merely a regime that watches individuals; it is an infrastructural form of power that pre-designs the environment in which action takes place, turns data production into a de facto condition of social existence, and governs subjects not by excluding them, but by forcibly including them within data networks. The article distinguishes the Onopticon from neighboring concepts such as the Panopticon, the surveillant assemblage, surveillance capitalism, and algorithmic governmentality, and defines the specific subject form produced by this regime as Homovictimus. Through the case of Aadhaar, it examines data compulsion and exclusionary inclusion, and positions Judea Pearl's Structural Causal Models as a powerful methodological tool for analyzing algorithmic exclusion. Finally, the article argues that legal transparency alone is insufficient and discusses Data Commons as a political horizon aimed at collective control over data.

Keywords: Onopticon; algorithmic power; Homovictimus; algorithmic governmentality; Structural Causal Models; Data Commons; Environment Configuration

1. Introduction: The Explanatory Crisis of Surveillance and the Infrastructural Turn

Bibliometric studies of surveillance-society scholarship show a double movement across the 1984-2023 ([K. Gökler](#)) period. On the one hand, the field consolidated around a powerful theoretical core shaped above all by Michel Foucault and David Lyon, especially after 2008. On the other hand, it expanded through themes such as security, privacy, big data, neoliberal governmentality, software-based sorting, and data-driven governance, thereby moving beyond the classical Panopticon as a sufficient explanatory model. This does not mean that

surveillance studies have weakened. It means that their founding metaphor has reached its explanatory limits.

A bibliometric note is in order: such mappings are useful for identifying the field's center of gravity, but they also risk underrepresenting adjacent literatures such as platform governance, STS, and critical data studies when the corpus is restricted to English-language social-science articles indexed under a narrow search term.

The bibliometric map itself, however, has clear limits. An archive restricted to English-language social-science articles indexed in Scopus under the phrase "surveillance society" inevitably leaves out substantial portions of the literature on platform governance, critical data studies, science and technology studies, and algorithmic management. Even so, the overall pattern is unmistakable: contemporary forms of digital power can no longer be fully explained through the vocabulary of watching, recording, and disciplining after the fact.

This article does not claim to discover a wholly untouched gap in the literature. Its contribution is different. It seeks to reorganize a dispersed set of post-panoptic, infrastructural, software-mediated, and data-intensive transformations under a single ontological schema. The name given to that schema is the Onopticon.

The article addresses three questions. First, why does the Panopticon no longer suffice as an explanatory model for contemporary algorithmic power? Second, what common ontological plane is provided by the concept of the Onopticon for transformations already discussed in fragmented ways across the literature? Third, how can the forms of structural exclusion generated by this regime be analyzed and causally tested?

The core thesis is that contemporary algorithmic power is defined less by the act of watching individuals than by the pre-design of the environment in which action becomes possible, by the narrowing of the field of options, and by the conversion of data production into a de facto condition of public existence. For that reason, we need a conceptual transition from the disciplinary logic of the Panopticon to an infrastructural logic of environment configuration. The Onopticon names that transition.

Five constitutive features define the Onopticon:

- 1) the transformation of data production from an individual preference into a practical condition of public and social existence;
- 2) the infrastructural design of action ex ante rather than its supervision after the fact;
- 3) the narrowing of the field of possibilities through algorithmic steering;
- 4) the operation of exclusion not through expulsion from the system but through compulsory inclusion within data networks; and
- 5) the application of power not primarily through legal texts but through code, standards, interfaces, protocols, and hardware.

2. Post-Panoptic Literature and the Conceptual Position of the Onopticon

The strength of the concept becomes visible only when its relation to neighboring concepts is stated precisely. The Panopticon refers to a regime of visibility in which the subject internalizes discipline under the assumption of being watched. This remains analytically useful for prisons, schools, barracks, and factories. Yet digital platforms, scoring systems, predictive rankings, and data-driven access regimes are not exhausted by the question of visibility. The decisive issue is the prior design of the option architecture through which subjects move.

The surveillant assemblage emphasizes the networked, fragmented, and distributed character of surveillance, but it does not sufficiently center the force of preconfigured environmental constraint. Surveillance capitalism powerfully captures the extraction and commodification of behavioral surplus, but its emphasis on market accumulation can understate the fused role of the state, public infrastructure, and access regimes. Algorithmic governmentality is crucial because it shows how governance operates through signals and traces independently of conscious intention. The Onopticon builds on that insight while shifting attention to the material and technical arrangement of the environment itself. Lessig's claim that code is law provides the legal and architectural backbone of this move, yet the Onopticon treats this not as a slogan but as a description of a whole regime in which technical conditions become socially binding norms.

The Onopticon therefore does not replace the existing literature. It concentrates its dispersed insights into a single ontological frame. Its analytical novelty lies in moving from explanations centered on surveillance to explanations centered on environment configuration.

Table 1. Distinguishing the Onopticon from neighboring concepts

Concept	Core Logic	Level of Operation	Relation to the Subject	Temporality	Difference from the Onopticon
Panopticon	Visibility, supervision, internalized discipline	Institutional and supervisory	Observed subject disciplining itself	After-the-fact correction / discipline	The Onopticon is concerned not only with visibility but with the prior configuration of the environment.
Surveillant assemblage	Networked, fragmented,	Data flows and heterogeneous networks	Fragmented data-subject	Continuous tracking	The Onopticon accepts networked surveillance but

	distributed surveillance				centers predesigned environmental constraint.
Surveillance capitalism	Extraction and commodification of behavioral surplus	Market and platform economy	Predicted and monetized user	Behavioral futures turned into value	The Onopticon addresses not only market extraction but also state infrastructure and access regimes.
Algorithmic governmentality	Governance through signals, traces, classification, optimization	Computation and probabilistic sorting	Data-subject processed independently of conscious intention	Predictive intervention	The Onopticon extends this insight to interfaces, standards, infrastructure, and hardware.
Onopticon	Ex ante environment design, data compulsion, narrowing of possibility	Code, interface, infrastructure, protocol, hardware	Compulsory data producer and classified subject	Preconfiguration	Its distinctive feature is to conceptualize power as environmental engineering rather than surveillance.

3. The Architectural Logic of the Onopticon: Environmental Engineering and Navigational Power

What distinguishes the Onopticon is the replacement of surveillance-and-correction with mechanisms of preconfiguration. In the classical panoptic order, power disciplines the subject by observing it. In the Onoptic order, architecture itself becomes the mode of power. Technical standards, interface design, access protocols, ranking systems, identity-verification procedures, and hardware restrictions do not literally replace law, but they come to govern everyday action more directly than law often does.

In that sense, the Onopticon is not merely a regime of “nudging.” In behavioral economics, a nudge lightly restructures a choice architecture while preserving the subject’s options in principle. The Onopticon operates at a different level. What is at stake is not just the presentation of options but the algorithmic narrowing of the options themselves. The subject

does not always confront an explicit prohibition; more often it encounters a corridor of precomputed routes. It is therefore more accurate to describe this form as navigational power. Navigational power does not wait to punish action. It determines in advance the limits within which action can become possible.

The political consequence is clear. Freedom is not neutralized only by prohibition. It can also be diminished through the technical management of possibility spaces. The subject appears to move freely, yet often moves only within an already sorted, optimized, and narrowed field of possible action.

4. Data Compulsion, Exclusionary Inclusion, and Homovictimus

The clearest feature of the Onoptic regime is data compulsion. In banking systems, digital public services, health infrastructures, communications systems, and mobile identity verification, abstaining from data production is rarely a simple technological preference. In many cases it amounts to relinquishing practical access to social life. Data production should therefore be understood not as voluntary participation but as a material precondition of public and economic existence.

This compulsion is not distributed evenly across the globe. In the Global North, data-based classification often operates through consumer profiling, creditworthiness, risk scoring, and platform ranking. In the Global South, biometric identification, digital registration, and welfare access can have much harsher consequences. This matters because the Onopticon is not merely a market logic for steering consumption; it is also an infrastructural logic for governing access to the means of life.

To describe the subject form produced by this regime, this article proposes the concept of Homovictimus. The term is not meant as a loose label for every digital user. It designates a more specific subject: one who is compelled to exist within data networks, whose public and economic existence depends on continuous data production, and who is then classified, ranked, and marginalized through that very datafication.

The key mechanism here is not exclusion in the old sense but exclusionary inclusion. The subject is not dominated because it has been expelled from the system; it is dominated because it is forcibly included at the center of the system. Agamben's Homo Sacer captured the exposure of bare life before sovereign power. Homovictimus captures a different paradox: the individual is simultaneously the compulsory producer of data and the one subjected to the classificatory violence of that data. Data thereby ceases to be a mere representational medium and becomes a practical determinant of social fate.

5. The Reflexivity Paradox and Algorithmic Resistance

The central epistemic problem of the Onopticon is that algorithms do not merely predict the future; they participate in producing the conditions under which that future will occur. When predictive systems intervene in credit, work, insurance, welfare, security, and visibility, they do not simply register social behavior. They help shape it. A performative feedback loop emerges in which the model both records and contributes to the behavior it claims to measure.

For that reason, the informational logic of the Onopticon is not merely representational. It is constitutive. The continuous optimization of narrow metrics such as click-through, engagement, retention, risk, and efficiency reshapes social reality around what can be measured. The problem is therefore not only mistaken prediction. It is also the technical reduction of value to what the system has decided to count.

Yet the picture is not wholly closed. A variety of algorithmic resistance practices have emerged against the closures built by Onoptic architecture. Data-obfuscation tools, open-source software, privacy-preserving protocols, and cryptographic communication networks offer micro-level tactics. At the collective level, platform workers' legal struggles against algorithmic management, demands for data access, challenges to automated decision-making, and experiments with data cooperatives show that this regime is politically contestable. Homovictimus is therefore not a purely passive figure. It is a subject whose agency is narrowed, but not abolished.

5.1. Weaponizing the Algorithm: Infrastructure and Environment Design in Contemporary War

The logic of the Onopticon is now visible not only in civil governance but also in contemporary war. Here, the algorithm is not reducible to a narrow notion of target-selection software. More broadly, algorithms fuse sensor feeds, construct a common operational picture, synchronize logistics, accelerate command cycles, and pre-structure the environment in which movement, detection, and destruction become possible. In this sense, the weaponization of the algorithm is not merely the automation of lethality; it is the transformation of the battlespace into a continuously computed environment. A 2025 U.S. Army account of the Maven Smart System describes it precisely in these infrastructural terms: as an AI-enabled system that combines sensors, machine learning, targeting, logistics planning, and supply prediction within one operational architecture.

The Russia-Ukraine war offers one of the clearest laboratories of this shift. A 2025 assessment by the Institute for the Study of War noted that, as of early June 2025, neither

Russia nor Ukraine had yet deployed fully AI/ML-enabled drone warfare at scale, but both were increasingly integrating machine-learning capabilities into new drone variants and battlefield adaptation cycles. Current reporting in March 2026 shows the next step in that process: Ukraine has begun opening battlefield data to allied states and companies so that AI models can be trained on millions of annotated images and combat flights. What is decisive here is not simply better targeting. The battlefield itself becomes a data infrastructure and a training environment - an operational space that is continuously re-modeled, re-visualized, and re-optimized while the war is still being fought.

The Israeli war in Gaza reveals a different but related configuration. Reuters reported in April 2024 that the United States was examining reports that Israel had used AI to help identify bombing targets in Gaza, while Human Rights Watch warned in September 2024 that the Israeli military's use of surveillance technologies, AI, and other digital tools to help determine who or what to attack may be increasing the risk of civilian harm. In this setting, algorithmic power does not only classify targets; it also helps structure movement, evacuation, density, and the timing of attack within a tightly controlled space. The significance of these systems therefore exceeds the question of whether a machine autonomously 'selects' a target. What matters is that data-intensive infrastructures increasingly shape the spatial and temporal conditions under which civilians and combatants are made visible, movable, stoppable, or strikeable.

The current U.S.-Iran confrontation makes visible the doctrinal side of this transformation. Official U.S. defense strategy already frames data, analytics, and AI as central to decision advantage, operational tempo, and integrated warfighting. Reporting from March 2026 on the U.S.-Israeli operation against Iran underscores how contemporary conflict is organized through distributed sensing, rapid decision cycles, alliance management, and digitally mediated battlespace coordination as much as through direct firepower. From this standpoint, the Onopticon in war is not exhausted by autonomous weapons. It names a broader condition in which sovereignty is exercised through the capacity to build the infrastructure of perception, prediction, synchronization, and intervention before force is applied. Contemporary warfare is therefore increasingly a problem of environment design: deciding what data will circulate, what will count as a threat, which actors will be rendered visible, and which operational pathways will remain open or closed.

6. Deep Case: Aadhaar and the Onopticon as Compulsory Inclusion

One of the clearest illustrations of the Onopticon is India's Aadhaar system. At first glance, Aadhaar appears as a technical digital identity infrastructure designed to improve administrative efficiency, reduce fraud, and rationalize the distribution of welfare. Its social effects, however, go far beyond a neutral identity-verification technology. Aadhaar has not simply digitized citizenship. It has become a practical gateway to public services, welfare provision, and, in some cases, the material means of survival.

Aadhaar clarifies the central claim of this article: contemporary power no longer operates only by watching individuals. It also preconfigures the environment through which individuals gain access to the conditions of life. The decisive issue is not whether the person is being observed at a given moment. It is whether recognition, service access, and social legibility are tied to a technical chain of verification. Once the receipt of aid, proof of identity, recognition by the system, and access to services depend on data production, data ceases to be an external record and becomes a condition of social existence.

The Onoptic character of Aadhaar can be seen on three levels. First, it turns data production into a precondition of public access. Individuals must produce biometric and demographic data not only to be recognized by the state, but also to secure access to aid, services, and mobility. Data production thus shifts from a voluntary digital act to a technical requirement for living within the social order.

Second, Aadhaar produces exclusion not by expelling subjects from the system but by including them under conditions they cannot control. Those who suffer exclusion are not simply outside the register. They are individuals compelled to enter the system whose inclusion fails when the technical conditions of inclusion fail. Biometric mismatches, data inconsistencies, connectivity failures, and administrative matching errors can all generate exclusion precisely because the person has been made dependent on the system's preferred mode of recognition. Exclusion therefore operates here as exclusionary inclusion.

Third, Aadhaar demonstrates how power functions at the level of infrastructure rather than solely at the level of formal legal text. The issue is not simply what the law says. It is whether the scanner works, whether the network connects, whether the database returns a match, and whether the verification protocol recognizes the subject. This extends Lessig's claim that code is law: not only code but the entire technical ecology in which code is embedded becomes norm-producing. Interface, device, protocol, and database jointly constitute a regime of power.

Aadhaar also renders the concept of Homovictimus empirically legible. The subject cannot be recognized within the system without producing data, yet the same process of datafication can expose that subject to technical failure, bureaucratic fragility, and deprivation of aid or access. The individual becomes less the owner of data than the victim of data. Social visibility is achieved through data, but that visibility no longer secures rights; it makes those rights conditional, interruptible, and revocable.

Aadhaar therefore shows that the Onopticon is not exhausted by privacy violation. The deeper issue is that the conditions of public existence are increasingly defined by infrastructures of technical verification. In that sense, Aadhaar is not merely a digital identity project. It is a paradigmatic Onoptic case in which data compulsion, exclusionary inclusion, and infrastructural domination converge.

6.1. The Geographic Flexibility of the Onopticon: Rigid and Fluid Infrastructures

When Aadhaar in India and algorithmic credit scoring in the West are read together, the Onopticon no longer appears as a uniform mechanism of domination. It reveals itself instead as a regime that adapts to geographical and socio-economic context. In the Global South, the Onopticon can take a more rigid form, closing directly around what Agamben called bare life. In the Aadhaar case, biometric compulsion becomes a gateway to food, shelter, welfare, and the material means of survival. Exclusionary inclusion here can generate immediate physical and life-sustaining threats.

By contrast, in the Global North, algorithmic credit scoring and platform governance often represent a more fluid form of the Onopticon. The individual is not typically confronted with direct hunger for failing to produce data. Instead, financial mobility, housing access, employment opportunities, and social status are narrowed algorithmically. Homovictim thus appears in India as a digital pariah compelled to submit biometric proof in order not to be cast out of the system, while in the United States or Europe the same figure appears as an indebted subject compelled to align consumption habits and behavioral traces with systemic rationalities in order to secure better credit, lower interest, or access to desirable neighborhoods.

These two cases indicate that the Onopticon governs both the material reproduction of life in the South and financial or social mobility in the North through the same infrastructural logic: the prior design of the field of options. The difference lies not in the disappearance of domination but in the density and immediacy of its consequences.

7. Analyzing Onoptic Exclusion: Structural Causal Models as a Test Instrument

To analyze the structural exclusions produced by the Onopticon, it is not enough to rely on data analytics built solely on correlations. The issue is not only that certain variables appear alongside certain outcomes. The deeper issue is that historically produced inequalities are reintroduced through variables that look neutral on the surface. Contemporary algorithmic exclusion must therefore be interrogated not only at the level of predictive performance, but at the level of causal structure.

In this context, Judea Pearl's Structural Causal Models offer a powerful analytical instrument for testing Onoptic exclusion beyond correlation. SCM is not the only valid method. Its value

lies in the fact that it enables counterfactual reasoning and thereby helps make visible the historical and social background conditions that inform seemingly neutral decisions.

Pearl's framework can be expressed as $M = \langle V, U, F, P(u) \rangle$, where V denotes observable endogenous variables, U denotes unobserved exogenous background variables, F denotes the structural functions linking variables, and $P(u)$ denotes the probability distribution of the unobserved variables. This distinction matters for social theory because algorithmic systems frequently claim to make objective decisions by using measurable indicators such as ZIP code, income, education, debt, interaction history, or behavioral traces. Yet those indicators may carry the sediment of racialized exclusion, class inequality, spatial segregation, or institutional discrimination. The contribution of SCM lies precisely in making the influence of that invisible background analytically legible.

7.1. SCM as a Tactic of Reverse Engineering and Exposure

At first glance, the article's post-structural, Foucauldian critique of power and Judea Pearl's Structural Causal Models may appear to belong to different epistemological universes. In this article, however, SCM is not positioned as a positivist device that claims to objectively model social totality. It is used tactically, as a method of reverse engineering capable of cracking the black box of Onoptic power.

The Onopticon typically hides the exclusions it produces behind the neutral mathematical surface of correlation. Decision-making algorithms rarely target historically disadvantaged groups explicitly. Instead, they rationalize exclusionary inclusion by relying on the residues left by invisible background variables, such as ZIP code, schooling history, or behavioral traces. For courts, civil-society organizations, and data activists, it is rarely enough to say that an algorithm is biased. That statement alone often fails to generate legal or political traction.

The counterfactual architecture provided by SCM makes it possible to expose historically sedimented inequalities in the very language that power itself claims as neutral: mathematics and data science. In this sense, SCM functions not merely as an analytic tool but also as an instrument of methodological resistance. It opens a way for Homovictimus to appear not only as a passive victim but also as a subject capable of decomposing and contesting the algorithmic violence exercised through its own data.

8. Case Analysis: Credit Scoring, ZIP Codes, and Causal Structure

Credit-scoring systems provide a revealing illustration of the Onopticon at work. Financial institutions frequently use residential area, income level, educational background, repayment history, and similar variables as indicators of risk. At first glance these may seem technical

and neutral. Yet variables such as ZIP code can function as proxies for historical discrimination and spatial inequality.

This can be visualized through a simplified directed acyclic graph. The system appears to issue a decision by using only observable variables such as ZIP code and income-education level. Yet behind those variables stand unobserved background conditions shaped by historical and structural inequality. The apparently neutral decision of the algorithm can therefore become a technical translation of prior regimes of exclusion.

The point is not simply that the model is biased. The deeper point is that socially produced exclusion is re-circulated in technical form. SCM does not offer an automatic solution here. Defining exogenous variables precisely and constructing their probability distributions remains difficult in social research. Even so, the framework provides an important methodological expansion because it reveals causal paths that correlation-based assessments often obscure.

Figure 1. Simplified DAG model of structural exclusion in algorithmic credit scoring

9. The Limits of Legal Resistance and the Illusion of Transparency

Public and legal responses to algorithmic regimes are frequently organized around demands for transparency. Calls for access to source code, explainability, disclosure of automated decisions, and administrative review are undoubtedly important. Yet from the standpoint of the Onopticon, the problem is not only that a decision is opaque. The deeper problem is that the infrastructure, data architecture, and causal logic that make the decision possible remain outside democratic scrutiny.

For that reason, opening source code is not sufficient by itself. Without access to training data, variable selection, target functions, optimization criteria, and the social outcomes deemed acceptable by the system, transparency can easily become a superficial instrument of legitimation. Similarly, the rhetoric of explainable AI often offers post hoc rationalizations rather than genuine access to the decision's causal structure.

Legal transparency struggles are therefore necessary but insufficient. Onoptic power operates not only at the level of code, but also at the level of data architecture, access infrastructure, standards, and ownership relations. The object of democratic control must accordingly extend beyond software decisions to the full set of infrastructural conditions that make those decisions possible.

Any political response to the Onopticon must therefore go beyond demands for visibility or explainability alone. The issue is not simply why a decision was made, but who built the infrastructure that made the decision possible, who governs it, and which social purposes it

is optimized to serve. The struggle is thus as much about architectural sovereignty as about legal transparency.

10. Conclusion: From Surveillance to Data Commons

This article has argued that the classical model of the Panopticon has become increasingly insufficient for explaining contemporary forms of algorithmic power and that it must be supplemented by a concept capable of capturing the prior design of environments. The proposed concept of the Onopticon seeks to gather dispersed discussions of software-based sorting, algorithmic governmentality, data colonialism, and infrastructural governance within a common ontological frame.

What distinguishes contemporary power in this account is not simply the observation of individuals, but the prior shaping of action spaces, the transformation of data production into a practical condition of public access, and the forcing of subjects into narrowed architectures of choice. The subject generated by this regime is Homovictimus: a figure compulsorily included within data networks and marginalized through that very inclusion.

The article has also suggested that Structural Causal Models provide an important methodological opening for the analysis of Onoptic exclusion. Their importance lies not in guaranteeing final truth, but in making it possible to ask how historical inequalities are technically reproduced under the appearance of neutral decision-making. Methodological clarification, however, does not itself constitute political resolution.

The decisive question is therefore no longer diagnosis alone, but institutional and material reorganization. Transparency regimes and legal oversight remain valuable, yet Onoptic domination cannot be meaningfully limited unless the ownership, circulation, and use of data are transformed. Data Commons should be understood not as a vague ethical wish, but as a political direction aimed at collective control over the infrastructures through which data is generated and used. The task is no longer only to criticize surveillance. It is to define the institutional and infrastructural principles through which more livable, more just, and more common digital environments can be built.

References

- Agamben, G. (1998). *Homo Sacer: Sovereign Power and Bare Life*. Stanford University Press.
- Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era*. University Press of Kansas.
- Bigo, D. (2006). Globalized (in)security: The field and the Ban-opticon. In D. Bigo & A. Tsoukala (Eds.), *Illiberal Practices of Liberal Regimes: The (In)security Games* (pp. 5-49). L'Harmattan.

- Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.
- Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Pantheon Books.
- Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault Effect: Studies in Governmentality* (pp. 87-104). University of Chicago Press.
- Graham, S. (2005). Software-sorted geographies. *Progress in Human Geography*, 29(5), 562-580.
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622.
- Khera, R. (Ed.). (2019). *Dissent on Aadhaar: Big Data Meets Big Brother*. Oxford University Press.
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press.
- Pearl, J. (2009). *Causality: Models, Reasoning, and Inference* (2nd ed.). Cambridge University Press.
- Rouvroy, A. (2013). The End(s) of Critique: Data Behaviourism versus Due Process. In M. Hildebrandt & K. de Vries (Eds.), *Privacy, Due Process and the Computational Turn* (pp. 143-167). Routledge.
- Stiegler, B. (2018). *The Neganthropocene*. Open Humanities Press.
- Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
- Justice K. S. Puttaswamy (Retd.) and Another v. Union of India and Others, Supreme Court of India (2018).
- Gökler, K. <https://dergipark.org.tr/tr/pub/@kubraagokler>

Human Rights Watch. (2024, September 10). Gaza: Israeli military's digital tools risk civilian harm.

Human Rights Watch. (2024, September 10). Questions and answers: Israeli military's use of digital tools in Gaza.

Reuters. (2024, April 4). U.S. looking at report that Israel used AI to identify bombing targets in Gaza.

Reuters. (2026, March 12). Ukraine opens battlefield data access to allies' AI models.

Reuters. (2026, March 17). Trump says NATO's refusal to help on Iran is a very foolish mistake.

Stepanenko, K. (2025, June). The battlefield AI revolution is not here yet: The status of current Russian and Ukrainian AI drone efforts.

U.S. Army. (2025, March 3). Contracting personnel use AI, Maven Smart System simulation during warfighter exercise.

U.S. Department of Defense. (2023). Data, analytics, and artificial intelligence adoption strategy.

U.S. Department of State. (2023). Political declaration on responsible military use of artificial intelligence and autonomy.